IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Minwen JI et al.	§	Confirmation No.:	6293
Serial No.:	10/716,588	§	Group Art Unit:	2135
Filed:	11/19/2003	§	Examiner:	T. B. Truong
For:	Electronic Message Authentication	§	Docket No.:	200311664-1

APPEAL BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Date: May 28, 2008

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on March 28, 2008.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, L.P. (HPDC), a Texas Limited Partnership, having its principal place of business in Houston, Texas. HPDC is a wholly owned affiliate of Hewlett-Packard Company (HPC). The Assignment from the inventors to HPDC was recorded on November 19, 2003, at Reel/Frame 014728/0745.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals or interferences.

III. STATUS OF THE CLAIMS

Originally filed claims:	1-18.
Claim cancellations:	9, 10 and 17-20.
Added claims:	19 and 20.
Presently pending claims:	1-8 and 11-16.
Presently appealed claims:	1-8 and 11-16.

IV. STATUS OF THE AMENDMENTS

Appellants filed a response to the final Office Action on March 25, 2008 to cancel claims 9-10 and 17-20, which had been previously withdrawn. In an Advisory Action dated April 23, 2008, the Examiner acknowledged the cancellation of claims 9-10 and 17-20.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the independent claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters as examples of support for claim elements, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claims.

As described in the Background of Appellants' specification, the amount of business activities conducted via the Internet is increasing. However, security protocols for conducting such activities may not provide sufficient reliability and security. Appellants' contribution identifies and addresses this problem.

For example, the invention of claim 1 is directed to a method that comprises calculating a first part of a message authentication function (DeHMAC2) by a first processor (118, Figure 1) and calculating a second part of the message authentication function (DeHMAC1) by a second processor (120, Figure 1).[1] The method further comprises combining the results of the first and second parts into a message authentication code (HMAC) by the first or second processors (118, 120).[2] The method further comprises using the message authentication code (HMAC) to authenticate data.[3]

The invention of claim 11 is directed to a system (100, Figure 1) that comprises a first processor (118, Figure 1) configured to compute a first part of a multi-part message authentication function (DeHMAC2) and a second processor (120, Figure 1) in communication with the first processor (118).[4] The second processor (120) is configured to compute a second part of the message

[1] See at least Figure 1 and lines 1-4 of paragraph [0021], page 7.

[2] See at least Figures 1-2 and lines 1-3 of paragraph [0024], page 8.

[3] See at least Figure 2 and lines 8-12 of paragraph [0022], page 11.

authentication function (DeHMAC1).[5] The first part of the message authentication function (DeHMAC2) is based on the contents of a record (*content* in equation 4) and the second part (DeHMAC1) is based on a data key (*secret* in equation 1).[6] The data key is inaccessible by the first processor (118) and the record contents are inaccessible by the second processor (120).[7]

[4] See at least Figure 1 and lines 1-4 of paragraph [0021], page 7.

[5] See at least Figure 1 and lines 1-4 of paragraph [0021], page 7.

[6] See at least lines 1-15 of paragraph [0022] and lines 1-4 of paragraph [0023], pages 7-8.

[7] See at least lines 7-11 of paragraph [0021], page 7.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-8 are directed to non-statutory subject matter under 35 U.S.C. § 101.

Whether claims 1-8 and 11-16 are anticipated by U.S. Patent App. Pub. No. 2002/0087818 A1 ("*Ripley*").

VII. ARGUMENT

A. § 101 Rejections of Claims 1-8

The Examiner argues that claim 1 only recites a mathematical calculation and therefore claim 1 and its dependent claims are unpatentable under 35 U.S.C. § 101. Appellants disagree for the following reasons. Claim 1 does not simply recite a mathematical calculation. Rather, claim 1 recites a decomposed message authentication code calculation having separate parts calculated by different processors. Further, claim 1 requires "using the message authentication code to authenticate data." As described in MPEP § 2106, a claim involving a mathematical algorithm is patentable if the final result of the claim is useful, tangible, and concrete. Appellants submit that the final result of claim 1 (*i.e.,* data security and authentication) is useful, tangible, and concrete as is required.

In an attempt to support the § 101 rejection, the Examiner appears to argue that the claimed limitation "using the message authentication code to authenticate data" would only involve intangible media (*e.g.,* signals or carrier waves) of a computer network. See Final Office Action dated 02/21/08, page 3, first paragraph. Appellants disagree at least because a computer network related to authenticating data as in claim 1 would involve at least some hardware components. Based on the foregoing, Appellants respectfully request that the rejection of claims 1-8 under § 101 be reversed and the claims set for issue.

B. § 102 Rejections of Claims 1-8 and 11-16

The Examiner rejected claims 1-8 and 11-16 as being anticipated by *Ripley*. Applicants disagree with the rejection because "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the...claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Claim 1 requires "calculating a first part of a message authentication function by a first processor" and "calculating a second part of the message

authentication function by a second processor." Claim 1 further requires "combining the results of the first and second parts into a message authentication code by the first or second processors." To support the § 102 rejection, the Examiner relies primarily on Figure 4 and paragraphs [0055]-[0057] of *Ripley*. However, Figure 4 and paragraphs [0055]-[0057] of *Ripley* clearly describe two separate MACs (a media MAC 73 and a reader MAC 75) instead of calculating two parts of a message authentication function as in claim 1 which results are combined into a message authentication code. As further evidence of this difference, *Ripley* describes comparing the two MACs rather than combining the results of the first and second parts of the message authentication function into a message authentication code. Based on the foregoing, Appellants respectfully submit that *Ripley* does not anticipate claim 1 and thus the § 102 rejection of claims 1-8 should be reversed and these claims set for issue.

Claim 11 requires "a first processor configured to compute a first part of a multi-part message authentication function" and "a second processor in communication with the first processor, the second processor is configured to compute a second part of the message authentication function." For much the same reasons as given with respect to claim 1, *Ripley* does not teach separate parts of a multi-part message authentication function computed by different processors as in claim 11.

Further, claim 11 requires "the first part of the message authentication function is based on the contents of a record and the second part is based on a data key, wherein the data key is inaccessible by the first processor and the record contents are inaccessible by the second processor." Just as *Ripley* does not teach the separate MAC parts of claim 11, *Ripley* does not teach that neither processor has access to all of the record content and/or keys related to the separate MAC parts as in claim 11. Based on the foregoing, Appellants respectfully submit that *Ripley* does not anticipate claim 11 and thus the § 102 rejection of claims 11-16 should be reversed and these claims set for issue.

C. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/Alan D. Christenson/

Alan D. Christenson
PTO Reg. No. 54,036
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400

VIII. CLAIMS APPENDIX

1. (Previously presented) A method, comprising:

calculating a first part of a message authentication function by a first processor;

calculating a second part of the message authentication function by a second processor;

combining the results of the first and second parts into a message authentication code by the first or second processors; and

using the message authentication code to authenticate data.

2. (Previously presented) The method of claim 1 wherein the message authentication code is used, in part, to authenticate data transmitted between the first processor and a third processor.

3. (Original) The method of claim 1 wherein the first and second processors are provided in separate computer systems.

4. (Original) The method of claim 1 wherein the first and second parts of the message authentication function consist of one-way hash functions.

5. (Original) The method of claim 1 wherein calculating the first part comprises calculating a value without having a data key associated with the function.

6. (Original) The method of claim 1 wherein calculating the second part comprises calculating a value for a data set without having contents of the data set.

7. (Previously presented) The method of claim 6 further comprising storing the contents into a non-volatile memory coupled to the first processor and storing

the message authentication code into non-volatile memory coupled to the second processor.

8. (Previously presented) The method of claim 1 further comprising calculating the message authentication code using the message authentication function on a data set, wherein the message authentication code can be used to authenticate a record that consists of the data set.

9.-10. (Canceled).

11. (Previously presented) A system, comprising:

a first processor configured to compute a first part of a multi-part message authentication function;

a second processor in communication with the first processor, the second processor is configured to compute a second part of the message authentication function;

wherein the first part of the message authentication function is based on the contents of a record and the second part is based on a data key, wherein the data key is inaccessible by the first processor and the record contents are inaccessible by the second processor.

12. (Original) The system of claim 11 wherein the message authentication function is used to authenticate data transmitted between the first processor and a third processor.

13. (Previously presented) The system of claim 11 wherein the second processor combines the message authentication function parts and provides the combined message authentication function result to the first processor to permit the first processor to authenticate the record with the combined message authentication function result and provide the authenticated record to a third processor.

14. (Original) The system of claim 11 wherein the first processor receives the second part from the second processor and encodes a record with the second part and transmits the encoded record to a third processor.

15. (Previously presented) The system of claim 11 wherein the first processor receives the record from a third processor, computes the first part of the message authentication function using contents of the record, and sends the result of the first part of the message authentication function and a message authentication code in the record to the second processor.

16. (Previously presented) The system of claim 11 wherein the second processor combines the message authentication function parts validates a message authentication code using the combined message authentication function.

17.-20. (Canceled).

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.